DOI: https://doi.org/10.37634/efp.2025.10.9
УДК 343.35:351.74 (477)

Євген Володимирович ***ШАПОВАЛЕНКО***
к.ю.н., доцент, Національна академія внутрішніх справ
ORCID: https://orcid.org/0000-0001-7973-686X
e-mail: navs-ord@ukr.net

Анатолій Анатолійович ***ОНІЩУК***
аспірант, Національна академія внутрішніх справ
ORCID: https://orcid.org/0009-0000-4575-3100
e-mail: anatoliionishchuk1355@gmail.com

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ ДБР ПРИВЛАСНЕННЮ, РОЗТРАТІ МАЙНА АБО ЗАВОЛОДІННЯ НИМ ШЛЯХОМ ЗЛОВЖИВАННЯ СЛУЖБОВИМ СТАНОВИЩЕМ, ЩО ВЧИНЯЄТЬСЯ ПОСАДОВИМИ ОСОБАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

У статті досліджено інформаційно-аналітичне забезпечення протидії оперативними підрозділами Державного бюро розслідувань привласненню, розтраті майна або заволодінню ним шляхом зловживання службовим становищем, що вчиняється посадовими особами Національної поліції України. Підкреслено, що результативність діяльності оперативних підрозділів безпосередньо залежить від своєчасного отримання, накопичення та оброблення оперативно значимої інформації стосовно факту вчинення злочину, його організаторів і співучасників, механізму протиправних дій, способів легалізації незаконних доходів і системи злочинних зв'язків.

Ключові слова: *привласнення, розтрата, майно, корупція, посадова особа, Національна поліція України, кримінальне правопорушення, оперативно-розшукова діяльність, протидія, оперативні підрозділи, Державне бюро розслідувань, інформаційне забезпечення, аналітичне забезпечення*

ВСТУП

Сучасний етап розвитку українського суспільства характеризується глибокими трансформаційними процесами у сфері державного управління та правоохоронної діяльності. В умовах воєнного стану, збройного конфлікту та постійних викликів, пов'язаних із за безпеченням національної безпеки, особливої ваги абувають питання ефективності протидії службовим злочинам, вчиненим посадовими особами Національної поліції України (НПУ). Зловживання службовим становищем, привласнення чи розтрата ввіреного майна підривають довіру суспільства до органів правопорядку, створюють корупційні ризики у секторі безпеки й оборони та безпосередньо впливають на обороноздатність держави.

У цьому контексті важливого значення набуває інформаційно-аналітичне забезпечення діяльності оперативних підрозділів Державного бюро розслідувань (ДБР). Саме воно є фундаментальною передумовою ефективного попередження, виявлення та документування злочинів, що посягають на державне майно або бюджетні ресурси. Своєчасне отримання та систематизація інформації про схеми привласнення чи розтрати, механізми легалізації незаконних доходів, коло причетних осіб і характер протиправних зв'язків дає змогу оперативним підрозділам не лише викривати злочинні дії, але й прогнозувати ризики їх поширення.

Проблематика інформаційно-аналітичного забезпечення протидії злочинам у сфері службової діяльності перебуває на перетині кримінального процесу, оперативно-розшукової діяльності та антикорупційної політики держави. Вона охоплює питання взаємодії між різними правоохоронними органами, застосування сучасних цифрових технологій, інтеграції інформаційних систем і захисту відомостей від несанкціонованого доступу. Недостатня врегульованість правових механізмів оброблення та використання інформації, а також фрагментарність наявних ресурсів створюють ризики зниження результативності діяльності ДБР у протидії службовим розкраданням.

Так, дослідження інформаційно-аналітичного забезпечення протидії оперативними підрозділами ДБР привласненню, розтраті чи заволодінню майном посадовими особами НПУ має не лише теоретичне, але й практичне значення. Воно спрямоване на вдосконалення підходів до збору, оброблення та використання інформації у кримінальних провадженнях, формування комплексної моделі міжвідомчої взаємодії та розроблення ефективних алгоритмів виявлення корупційних ризиків у діяльності поліції.

МЕТА статті – науково-практичне обґрунтування ролі та значення інформаційно-аналітичного забезпечення у діяльності оперативних підрозділів ДБР, спрямованої на виявлення, документування та попередження привласнення, розтрати чи заволодіння майном шляхом зловживання службовим становищем посадовими особами НПУ.

МЕТОДИ ДОСЛІДЖЕННЯ

Методологічну основу дослідження становить поєднання загальнонаукових і спеціально-правових методів. Формально-правовий метод застосовано для вивчення змісту Закону та суміжних нормативно-правових актів. Системно-структурний метод – для розкриття комплексу пошуково-аналітичних заходів, які здійснюються під час документування кримінальних правопорушень привласненню, розтраті майна або заволодінню ним шляхом зловживання службовим становищем, що вчиняється посадовими особами НПУ. Методи аналізу і синтезу дають змогу узагальнити наукові підходи та сформулювати висновки про оновлення оперативно-розшукового законодавства та прийняття спеціального відомчого акту для порядку накопичення, збереження та використання даних, отриманих у ході оперативно-

розшукової діяльності.

РЕЗУЛЬТАТИ

Інформаційно-аналітичне забезпечення протидії привласненню, розтраті майна або заволодінню ним шляхом зловживання службовим становищем, що вчиняється посадовими особами НПУ, є ключовим елементом діяльності оперативних підрозділів ДБР. Його значення обумовлюється як високим рівнем латентності цих кримінальних правопорушень, так і складністю виявлення корупційних діянь, вчинених особами, які володіють спеціальними знаннями, мають доступ до конфіденційної інформації та володіють ресурсами для приховування злочинної діяльності.

Впровадження сучасних інформаційно-аналітичних систем, зокрема в діяльність правоохоронних структур, відкриває нові перспективи для оброблення, інтерпретації та використання великих масивів не структурованих даних. Водночас криміногенне середовище також зазнає змін: кримінальні структури дедалі активніше інтегрують до своєї протиправної діяльності найновіші досягнення науки і техніки, комп'ютерні технології та засоби кібервпливу, що особливо помітно у сфері діяльності правоохоронних органів [1, с. 50]. Як слушно зазначає Л.І. Аркуша, вирішальне значення в ухваленні рішень у будь-якій сфері діяльності має рівень поінформованості суб'єкта, уповноваженого законом на їх прийняття. Вчена підкреслює, що в діяльності правоохоронних органів інформованість набуває особливої ваги, оскільки саме з визначення інформації, яка має значення для виявлення кримінальних правопорушень і встановлення місцезнаходження різних категорій осіб, починається розроблення та реалізація комплексу заходів протидії. У цьому контексті інформаційно-аналітичне забезпечення є не лише інструментом накопичення та систематизації даних, а й основою для формування тактичних і стратегічних рішень, що забезпечують ефективність діяльності оперативних підрозділів [2, с. 110].

Інформаційне забезпечення у сфері протидії злочинності розглядається як цілеспрямоване впровадження спеціалізованих засобів, що сприяють ефективному виявленню, дослідженню та документуванню джерел інформації відповідно до вимог законодавства, з метою формування доказів стосовно обставин учинення кримінальних правопорушень, способів їх здійснення та подальшого використання зібраних даних у кримінальному провадженні. На досудових стадіях воно передбачає постійний аналіз слідчої та оперативної практики, виявлення проблемних аспектів, їх наукове осмислення та нормативне, методичне й організаційне вирішення [3, с. 24].

Діяльність оперативних підрозділів ДБР з протидії привласненню, розтраті майна або заволодінню ним шляхом зловживання службовим становищем, має чітко виражений оперативно-розшуковий характер (ОРД). Основним завданням ОРД [4] у цій сфері є виявлення та фіксація відомостей про корупційно-мотивовану злочинну діяльність окремих посадових осіб та організованих груп у структурі НПУ. Як зазначає О.М. Бандурка, ОРД спрямовано на одержання інформації, її накопичення, аналітичне опрацювання та реалізацію результатів у формі конкретних заходів протидії; водночас всебічне висвітлення діяльності суб'єкта правопорушення є запорукою успішного припинення його протиправної поведінки [5, с. 281].

Інформаційно-аналітичне забезпечення є не лише інструментом оперативного реагування, але й базою для довгострокових стратегій протидії службовим розкраданням у НПУ. Аналітика розглядається як цілісна система принципів методологічного, організаційного та технологічного забезпечення індивідуальної й колективної інтелектуальної діяльності, що забезпечує ефективне оброблення інформації для виявлення її сутнісно-смислового ядра, підвищення якості наявних і набуття нових знань, а також формування інформаційної бази для ухвалення оптимальних управлінських рішень [6, с. 26].

Зміст аналітичного забезпечення ОРД включає: акумулювання оперативної інформації, одержаної під час виконання функціональних завдань; забезпечення доступу оперативних підрозділів до зовнішніх і внутрішніх інформаційних ресурсів; створення, інтеграцію та експлуатацію інформаційно-пошукових систем, баз і банків даних; впровадження аналітичних інструментів для своєчасного реагування на загрози.

Основні інформаційні джерела, що застосовуються в інформаційно-аналітичній діяльності ОРД: оперативні обліки; банки даних інформації, які формуються для комплексного аналізу криміногенної ситуації, дослідження динаміки і структури злочинності, визначення кримінологічних закономірностей і тенденцій, а також для планування превентивних заходів; банки даних правоохоронних органів, міністерств, відомств, підприємств, установ та організацій, міських і обласних органів влади; інформація приватних охоронних агентств; медіа-джерела. Застосування зазначених джерел у комплексі забезпечує оперативні підрозділи всебічною, достовірною та актуальною інформацією, що є підґрунтям для ефективного проведення аналітичної роботи, своєчасного ухвалення управлінських рішень та підвищення результативності протидії кримінальним правопорушенням.

Загалом інформаційно-аналітичне забезпечення ДБР у сфері протидії внутрішній корупції та службовим зловживанням в НПУ виконує дві взаємопов'язані функції:

1. Оперативну – забезпечення швидкого реагування на виявлені загрози, включаючи формування доказової бази та координацію дій із іншими органами (НАЗК, НАБУ, прокуратура).

2. Стратегічну – формування комплексної, довгострокової стратегії випереджувального впливу, яка враховує динаміку криміногенної ситуації, особливості воєнного стану, мобільність злочинних груп та специфіку службової діяльності поліцейських у зоні підвищених ризиків.

Як зазначає В.І. Школьніков, сьогодні є чимало аналітичних технологій як сукупність типових прийомів пошуку, оброблення та аналізу оперативно-розшукової інформації в інформаційних системах за допомогою спеціалізованих та інших програмно-технічних засобів з метою протидії протиправним діям окремих осіб та злочинних угруповань для виконання завдань з попередження злочинів та розшуку злочинців, а також виконання супутніх завдань з профілактики злочинності та прогнозування оперативної обстановки на певній території [7, с. 301]. Розвиток аналітичних технологій привів до появи інноваційних форм організації оперативної роботи та створення спеціалізованих підрозділів аналітичного спрямування.

Водночас «фундаментом» інформаційно-аналітичного забезпечення правоохоронної діяльності є кримінальний аналіз, який тісно пов'язаний з поняттям «великі дані», що є предметом цього аналізу [8, с. 198]. На думку С.В. Албула, кримінальний аналіз – це діяльність працівників правоохоронних органів, що полягає у пошуку, збиранні, перевірці, оцінюванні та обробленні оперативно-розшукової, доказової, криміналістичної та кримінологічної інформації, а також у встановленні за допомогою аналітичних технологій взаємозв'язків між подіями, особами, предметами тощо з метою вироблення нового знання для підвищення ефективності роботи з попередження, розкриття та розслідування кримінальних правопорушень й прогнозування злочинності [10, с. 35].

Предметом кримінального аналізу є обставини вчинення злочинів певних категорій, а також злочинність як явище. Зазначені відомості оперативний працівник одержує шляхом пошуку та збирання інформації оперативно-розшукового, доказового, кримінологічного та криміналістичного характеру з різноманітних несистематизованих джерел, її оброблення з метою приведення до форми, придатної для аналізу, а також безпосереднього аналізу інформації про певні злочини та злочинність з метою виявлення закономірностей. У ході збирання інформації оперативний працівник проводить її перевірку та оцінює вірогідність [8, с. 301]. Метою кримінального аналізу є виявлення неявних і прихованих зв'язків між фактами, подіями і особами з подальшим формулюванням версій і гіпотез для розкриття злочину [11, с. 37]. Метою кримінального аналізу може бути також запобігання кримінальним правопорушенням у рамках протидії злочинності, а також прогнозування злочинності на певній території оперативного обслуговування для здійснення профілактичного впливу на оперативну обстановку. Очевидно, що мету кримінального аналізу не може бути реалізовано без застосування аналітичних технологій, за допомогою яких можливо отримати якісно нову інформацію за результатами проходження первинними даними аналітичного циклу з метою попередження, розкриття та прогнозування злочинності.

Основними видами кримінального аналізу з урахуванням характеру та джерела інформації, застосованих аналітичних технологій та результатів такого аналізу, регулярності та частоти аналізу, а також цільової аудиторії та мети здійснюваного аналізу [12, с. 9]: аналітична кримінальна розвідка; тактичний кримінальний аналіз; стратегічний кримінальний аналіз; адміністративний (управлінський) кримінальний аналіз.

У межах аналітичної кримінальної розвідки вітчизняні фахівці виокремлюють й оперативний кримінальний аналіз – це процес, за яким аналітичні дослідження здійснюються з використанням всієї наявної інформації, а їхні результати надаються правоохоронним органам з метою використання для планування та проведення оперативно-розшукових заходів та операцій, а також слідчих (розшукових) дій [8].

Окрім тактичного значення, кримінальний аналіз є аналітичною платформою для підготовки управлінських рішень стратегічного рівня, доповідей, зведень, орієнтувань, довідок та профілів потенційно небезпечних осіб або груп [13].

Однією з найбільш дієвих методичних моделей, застосовуваних у навчанні та практиці кримінального аналізу, є «5W+H» (Who, What, When, Where, Why, How), що дає змогу системно структурувати дані, визначати коло причетних осіб, хронологію та географію подій, мотиви та способи вчинення злочинів [14, с. 149; 15, с. 159].

Кримінальний аналіз у межах протидії привласненню, розтраті майна або заволодіння ним шляхом зловживання службовим становищем, що вчиняється посадовими особами НПУ може здійснюватися на шести взаємопов'язаних етапах:

1. Планування та визначення цілей – постановка кон-кретних завдань, пов'язаних із виявленням службових зловживань.

2. Збирання інформації – одержання відомостей з відкритих, оперативно-розшукових, розвідувальних, відомчих та зовнішніх джерел, зокрема під час роботи в зонах бойових дій чи на деокупованих територіях.

3. Оброблення інформації – стандартизація, кодування та інтеграція даних для подальшого аналізу.

4. Аналіз інформації – виявлення схем, зв'язків, каналів руху ресурсів, способів маскування правопорушень.

5. Поширення інформації – підготовка аналітичних довідок, зведень, орієнтувань, що спрямовуються оперативним підрозділам та керівництву.

6. Повторне оцінювання – перевірка результативності аналізу, коригування методик, виявлення нових ризиків.

Джерела інформації включають результати періодичних та тематичних аналізів, дані з баз ДБР, інших правоохоронних органів, органів фінансового та податкового контролю, медіа, громадських платформ, а також результати OSINT-досліджень. Особливу увагу приділено профілюванню об'єктів, що мають підвищений ризик зловживань, із визначенням характерних деталей і сценаріїв їхньої діяльності.

Ключові інструменти кримінального аналізу ДБР:

– Аналіз зв'язків та візуалізація: *IBM i2 Analyst's Notebook* – побудова мережевих структур злочинних схем, виявлення посередників, аналіз часових послідовностей подій; *Maltego* – OSINT-розвідка, побудова цифрових профілів осіб, аналіз зв'язків у соцмережах і доменних структурах.

– Оброблення та аналіз даних: *Excel/Power Query/ Power Pivot* – робота з великими масивами транзакцій, телефонних з'єднань, службових журналів; *Power BI* – інтерактивні панелі, виявлення аномалій у фінансових потоках.

– Геоаналітика: *ArcGIS/QGIS* – відображення переміщень фігурантів, зон ризику, маршрутів поставок, зокрема у прифронтових районах.

– OSINT-інструменти: *Social Links, Skopenow, Spiderfoot* – пошук відкритих даних про майновий стан, ділові зв'язки та приховані контакти підозрюваних; фінансовий аналіз: виявлення компаній-прокладок, розкладання транзакцій за схемами, виявлення фіктивних контрактів.

– Відеоаналітика: *BriefCam* – аналіз відео з камер, ідентифікація транспортних засобів, переміщень осіб, фіксація фактів передачі ресурсів.

– AI/ML-рішення: *Palantir Gotham* – інтеграція різнорідних джерел, автоматична класифікація операцій за рівнем ризику.

– Документування та звітність: системи управління справами, шаблони звітів, стандартизоване включення діаграм та карт у матеріали кримінальних проваджень.

Впровадження технологій ШІ у роботу ДБР є важливим інструментом підвищення ефективності виявлення, документування та запобігання службовим розкраданням у НПУ, особливо в умовах воєнного стану та збройного конфлікту. ШІ дає змогу значно скоротити час на оброблення великих обсягів інформації, виявлення прихованих закономірностей та формування прогнозних моделей розвитку криміногенної ситуації.

1. Інтелектуальне обробленнф великих даних (Big Data). Застосування алгоритмів машинного навчання уможливлює: автоматичну класифікацію транзакцій та комунікацій за рівнем ризику; виявлення аномальних патернів у фінансових потоках, переміщенні матеріальних ресурсів та службовій кореспонденції; інтеграцію різнорідних джерел даних (відомчі бази, OSINT, результати негласних слідчих дій, аналітика громадських платформ). Це дає змогу формувати динамічні профілі підозрюваних з урахуванням службової поведінки, кола контактів та цифрових слідів.

2. Прогнозна аналітика та оцінювання ризиків. Моделі на основі глибинного навчання застосовуються для: прогнозування ймовірності зловживання владними повноваженнями у конкретних підрозділах НПУ; моделювання сценаріїв розвитку кримінальних схем у сфері службової діяльності; визначення «гарячих точок» (hot spots) з підвищеною концентрацією корупційних ризиків. У воєнний час особливу роль відіграє прогнозування ризиків у підрозділах, що працюють у прифронтових або деокупованих районах, де рівень зовнішнього контролю обмежений.

3. Автоматизований OSINT та цифрове профілювання [16]. ШІ-технології дають змогу: здійснювати безперервний моніторинг відкритих джерел, включно з соціальними мережами, месенджерами та даркнет-майданчиками; ідентифікувати фейкові акаунти, мережеві ботоферми та канали поширення незаконних пропозицій; аналізувати зв'язки між цифровими ідентифікаторами (IP-адреси, номери телефонів, адреси електронної пошти, криптовалютні гаманці).

4. Інтелектуальна відеоаналітика. Завдяки комп'ютерному зору ШІ застосовується для: розпізнавання облич, номерних знаків транспортних засобів та інших ідентифікаторів; аналізу поведінки об'єктів на відео (наприклад, повторювані зустрічі працівників поліції з певними особами); побудови часових ліній подій та реконструкції маршрутів переміщення підозрюваних.

5. Ризики та етичні аспекти застосування ШІ. В умовах воєнного стану надмірне застосування ШІ без належного контролю може призвести до: технологічної упередженості алгоритмів; надмірного втручання у приватне життя; маніпуляцій з боку осіб, що мають доступ до алгоритмічних моделей. Тому впровадження ШІ має супроводжуватися незалежним аудитом алгоритмів, захистом персональних даних та розробленням внутрішніх стандартів їхнього етичного застосування.

Підводячи підсумки підрозділу наголосимо, що інформаційно-аналітичне забезпечення діяльності оперативних підрозділів ДБР у сфері протидії привласненню, розтраті майна або заволодінню ним шляхом зловживання службовим становищем, вчинюваному посадовими особами НПУ, є ключовим складником сучасної системи протидії корупційної злочинності. Така діяльність є комплексним, багаторівневим процесом, який поєднує накопичення, оброблення, аналіз та застосування інформаційних ресурсів для підтримки ОРД, залежить від комплексного поєднання традиційних методів оперативно-розшукової роботи з інноваційними інструментами кримінального аналізу, включаючи ШІ-технології, автоматизоване оброблення великих масивів даних, прогнозовану аналітику та цифрове профілювання.

В умовах воєнного стану та збройного конфлікту значення аналітичного складника зростає у зв'язку з посиленням латентності службових розкрадань, ускладненням збору доказової інформації та необхідністю швидкого реагування на динамічні зміни у службово-корупційному середовищі поліції. ШІ та автоматизовані аналітичні системи забезпечують оперативне виявлення аномальних фінансових операцій, прихованих зв'язків між суб'єктами, ризикових зон та осередків потенційних зловживань, що особливо важливо у прифронтових і деокупованих територіях.

Водночас виявлено низку проблем, які гальмують повну реалізацію потенціалу інформаційно-аналітичного забезпечення: фрагментарність баз даних, обмежений доступ до зовнішніх джерел (зокрема фінансово-податкової аналітики), недостатня підготовка персоналу у сфері кіберрозвідки та прогнозування, низький рівень інтегрованості ІТ-рішень у систему ДБР. Відтак, гостро постало питання забезпечення інформаційно-аналітичним інструментом оперативні підрозділи ДБР як стратегічний напрям, що формує основу для запобігання, виявлення корупційних майнових злочинів у НПУ, а його розвиток та вдосконалення в умовах сучасних безпекових викликів є необхідною передумовою зміцнення верховенства права, прозорості та підзвітності правоохоронної системи України.

ВИСНОВКИ

Основним елементом організації пошукової діяльності та документування є інформаційно-аналітичне забезпечення, яке у контексті корупційної злочинності серед працівників НПУ має подвійне значення: по-перше, як складник організації діяльності – у формі оцінювання криміногенної та оперативної обстановки на об'єкті обслуговування, виявлення організованих форм злочинної діяльності, корупційних фактів; по-друге, як інструмент оцінювання, відбору та планування оперативно-тактичних заходів протидії, що здійснюються органами ДБР. В умовах збройного конфлікту та воєнного стану, ефективним для оперативних підрозділів ДБР є застосування можливостей кримінальної розвідки із застосуванням сучасних інструментів кримінального аналізу (IBM i2 Analyst's Notebook; Maltego; Microsoft Excel / Power Query / Power Pivot; Power BI; ArcGIS / QGIS; GeoTim; Social Links, Skopenow, Spiderfoot; IntelTechniques Tools; Palantir Gotham; Brief-Cam; Clearview AI; NLP-алгоритми; Case Management Systems), що забезпечують пошук акаунтів у соцмережах, ідентифікацію прихованих зв'язків, аналіз фінансових потоків, геоаналітику, відеоаналітику та документування результатів. Додатковими чинниками підвищення ефективності є взаємодія з інформаційними ресурсами інших правоохоронних органів та організація цільових тренінгів для працівників ДБР у межах системи спеціальної підготовки та підвищення кваліфікації.

Список використаних джерел

1. Максименко Ю.Є. Боротьба з тероризмом в умовах інформатизації. *Правові проблеми сучасності.* 2013. С. 48–50.
2. Аркуша Л.І. Проблеми взаємодії та інформаційного забезпечення правоохоронних органів у боротьбі з економічною організованою злочинною діяльністю. *Інформаційне забезпечення протидії організованій злочинності.* 2003. С. 109–117.
3. Збірник актів нормативно-правового регулювання фінансово-економічної безпеки / упоряд.: О.М. Кубецька та ін. Дніпро, 2019. 312 с.
4. Бесчастний В.М. Напрями удосконалення інформаційного забезпечення у протидії злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2016. № 1 (36). С. 24–28.
5. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
6. Бандурка О.М. Оперативно-розшукова діяльність. Харків, 2002. Ч. 1. 336 с.
7. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України*:* монографія / О. Користін та ін. Київ, 2024. 444 с.
8. Школьніков В.І. Використання методу кримінального аналізу для протидії організованій злочинності. *Часопис Київського університету права.* 2017. № 1. С. 300–303.
9. Рудий Т.В., Кулешник Я.Ф., Ярован С.В. Практика кримінального аналізу у протидії кіберзлочинності. *Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції*: матеріали Всеукр. наук.-практ. конф. (Львів, 23 берез. 2018 р.). Львів, 2018. С. 194–202.
10. Албул С.В. Методологія кримінальної розвідки: теоретико-праксеологічний дискурс. *Південноукраїнський правничий часопис.* 2016. № 2. С. 34–37.
11. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «RICAS» / Д.Ю. Узлов та ін. Харків, 2018. 90 с.
12. LeBlanc J. et al. Definition and Types of Crime Analysis. Standards, Methods, & Technology. *Overland Park, KS: International Association of Crime Analysts*, 2014. P. 9.
13. Мишко В.В. Інформаційно-аналітична робота у кримінальній розвідці. *Південноукраїнський правничий часопис.* 2016. № 2. С. 52–55.
14. Rossy Q., Ribaux O. A Collaborative Approach for Incorporating Forensic Case Data into Crime Investigation Using Criminal Intelligence Analysis and Visualisation. *Science & Justice.* 2014. № 54 (2). pp. 146–153.
15. Албул С.В., Користін О.Є. Концепція розвитку кримінальної розвідки органів внутрішніх справ України. *Південноукраїнський правничий часопис.* 2015. № 1. С. 158–163.
16. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень. Одеса, 2024. 180 с.

References

1. Maksymenko Y.Y. The fight against terrorism in the conditions of informatization. *Legal problems of modernity*, 2013. p. 48-50. (in Ukrainian).
2. Arkusha L.I. Problems of interaction and information support of law enforcement agencies in the fight against economic organized criminal activity. Information support for countering organized crime. 2003. pp. 109-117. (in Ukrainian).
3. Collection of acts of normative-legal regulation of financial and economic security / O.M. Kubetska et al. Dnipro, 2019. 312 p. (in Ukrainian).
4. Beschastnyi V.M. Directions for improving information support in countering crime. *The fight against organized crime and corruption (theory and practice)*. 2016. Vol. 1 (36), pp. 24-28. (in Ukrainian).
5. On Operational and Search Activity: Law of Ukraine No. 2135-XII of February 18, 1992. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (in Ukrainian).
6. Bandurka O.M. Operational and Search Activity. Kharkiv, 2002. Part 1. 336 p. (in Ukrainian).
7. Implementation of the "Intelligence-led Policing" philosophy in the criminal analysis system of the National Police of Ukraine: Monograph / O. Korystin et al. Kyiv, 2024. (444 p.). (in Ukrainian).
8. Shkolnikov V.I. Using the criminal analysis method to counter organized crime. *Journal of the Kyiv University of Law*. 2017. Issue 1. pp. 300–303. (in Ukrainian).
9. Rudyi T.V., Kuleshnyk Y.F., Yarovan S.V. The practice of criminal analysis in countering cybercrime. In *Information and analytical support for the activities of criminal police units*: Materials of the All-Ukrainian Scientific and Practical Conference (Lviv, March 23, 2018). Lviv, 2018. pp. 194-202. (in Ukrainian).
10. Albul S.V. Methodology of criminal intelligence: Theoretical and praxeological discourse. South Ukrainian Law Journal. 2016. Vol. 2. pp. 34–37. (in Ukrainian).
11. Applied criminal analysis based on the "RICAS" information and analytical system / D.Yu. Uzlov et al. Kharkiv, 2018. 90 p. (in Ukrainian).
12. LeBlanc J. et al. Definition and Types of Crime Analysis. Standards, Methods, & Technology. *Overland Park, KS: International Association of Crime Analysts*, 2014. P. 9.
13. Myshko V.V. Information and analytical work in criminal intelligence. *South Ukrainian Law Journal.* 2016. Vol. 2. pp. 52-55. (in Ukrainian).
14. Rossy Q., Ribaux O. A Collaborative Approach for Incorporating Forensic Case Data into Crime Investigation Using Criminal Intelligence Analysis and Visualisation. *Science & Justice.* 2014. № 54 (2). pp. 146–153.
15. Albul S.V., Korystin O.Y. The concept of criminal intelligence development in the internal affairs bodies of Ukraine. *South Ukrainian Law Journal.* 2015. № 1. pp. 158-163. (in Ukrainian).
16. Torbas O.O. OSINT in the investigation of criminal offenses. Odesa, 2024. 180 p. (in Ukrainian).

Yevhen SHAPOVALENKO
PhD in Legal Sciences, Associate Professor, National academy of internal affairs
ORCID: https://orcid.org/0000-0001-7973-686X
e-mail: navs-ord@ukr.net

Anatolii ONISHCHUK
postgraduate student, National Academy of Internal Affairs
ORCID: https://orcid.org/0009-0000-4575-3100
e-mail: anatoliionishchuk1355@gmail.com

INFORMATION AND ANALYTICAL SUPPORT FOR THE COUNTERACTION BY SBI OPERATIONAL UNITS TO THE MISAPPROPRIATION, EMBEZZLEMENT, OR TAKING POSSESSION OF PROPERTY THROUGH ABUSE OF OFFICIAL POSITION COMMITTED BY NATIONAL POLICE OFFICIALS

The paper examines the information and analytical support for the counteraction by the operational units of the State Bureau of Investigation (SBI) to the misappropriation, embezzlement, or taking possession of property through abuse of official position committed by officials of the National Police of Ukraine.

It is emphasized that the effectiveness of the operational units' activities directly depends on the timely acquisition, accumulation, and processing of operationally significant information regarding the committed crime, its organizers and accomplices, the mechanism of illegal actions, methods of legalizing illicit proceeds, and the system of criminal connections. Information support is viewed as a targeted complex of search and analytical measures aimed at preventing and suppressing criminal manifestations, systematizing and verifying intelligence, forming and utilizing information resources, and developing and applying algorithms for searching, verification, and forecasting. The analytical component includes comparing primary and additionally obtained data, assessing risks, modeling scenarios for the development of the operational situation, and planning and coordinating operational and search measures.

It is established that the lack of a unified regulatory framework for the use of information resources necessitates the updating of operational and search legislation and the adoption of a specific departmental act regarding the procedure for the accumulation, storage, and use of data obtained during operational and search activities and during the execution of assignments from the investigator or prosecutor for conducting covert investigative (search) actions using modern information and analytical technologies.

Keywords: *Misappropriation, embezzlement, property, corruption, official, National Police of Ukraine, criminal offense, operational and search activity, counteraction, operational units, State Bureau of Investigation, information support, analytical support*